I FW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Paul M. Agbabian		
Assignee:	Symantec Corporation		
Title:	A SECURITY MANAGEMENT SYSTEM INCLUDING FEEDBACK AND CONTROL		
Serial No.:	10/660,225	Filed:	September 10, 2003
Examiner:	Unknown	Group Art Unit:	2832
Docket No.:	SYMC1001		

Monterey, CA
June 15, 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner:

U.S. PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	NAME
1)	5,893,083	04/06/99	Eshghi et al.
2)	6,266,773 B1	07/24/01	Kisor et al.
3)	6,298,445 B1	10/02/01	Shostack et al.
4)	6,321,338 B1	11/20/01	Porras et al.
5)	6,484,203 B1	11/19/02	Porras et al.

OTHER DOCUMENTS

1)	Barrus, J., *“Intrusion Detection in Real Time in a Multi-Node, Multi-Host Environment”*, Master's Thesis, Naval Postgraduate School, Monterey, CA, i-xii, pp. 1-79, September 1997.
2)	Houston, G. et al., U.S. Patent Publication No. US-2002/0019945-A1, published on February 14, 2002, entitled “SYSTEM AND METHOD FOR MANAGING SECURITY EVENTS ON A NETWORK”, 29 pgs.
3)	*“SNIA CIM Interoperability Demonstration Backgrounder”*, Storage Networking Industry Association, pp. 1-2, 2002.
4)	*“SNIA Storage Management Initiative CIM/WBEM Technology Backgrounder”*, Storage Networking Industry Association, pp. 1-2, 2002.
5)	Hughes, K. and Wohlferd, D., *"Say Goodbye to Quirky APIs: Building a WMI Provider to Expose Your Object Info"*, pp. 1-16 [online]. Retrieved on December 24, 2002. Retrieved from the internet: URL:http://msdn.microsoft.com/msdnmag/issues/0500/wmiprov/print.asp.
6)	*“Common Information Model (CIM) Specification”*, Version 2.2, Distributed Management Task Force, Inc., Portland, OR, pp. I-VI, 1-97, June 14, 1999.
7)	Davis, J., *“WBEM Services Specification JSR-0048”*, Java One, Sun's 2001 Worldwide Java Developer Conference, pp. 1-19, 2001.
8)	Bhat, G., *“WBEM Services API and Examples”*, Java One, Sun's 2001 Worldwide Java Developer Conference, pp. 20-29, 2001.
9)	Westerinen, A., *“Modeling Information In CIM”*, Java One, Sun's 2001 Worldwide Java Developer Conference, pp. 31-43, 2001.
10)	Ptacek, T. and Newsham, T., *“Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”*, Secure Networks, Inc., pp. 1-63, January 1998.
11)	Yang, J., Ning, P., Wang, X., and Jajodia, S., *“Cards: A Distributed System For Detecting Coordinated Attacks”*, Center for Secure Information Systems, George Mason University, Fairfax, VA, pp. 1-10.
12)	Magers, D., *“Packet Sniffing: An Integral Part of Network Defense”*, 9 pgs., May 9, 2002.
13)	King, N. and Weiss, E., *“Network Forensics Analysis Tools (NFATs) Reveal Insecurities, Turn Sysadmins Into Systems Detectives”*, Information Security, 8 pgs., February 2002.
14)	Trenum, G., *“Practical Requirement for Level 2 IDIC Exam”*, 15 pgs.
15)	Shimomura, T., *“Tsutomu Shimomura's Newsgroup Posting With Technical Detail of the Attack Described by Markoff in NYT”*, Random Access, 10 pgs., October 12, 1997.
16)	*“Dragon 5, An Intrusion Detection System for the Enterprise”*, 5 pgs.

17)	Stevens, W., The Protocols, TCP/IP Illustrated, Volume 1, Addison Wesley Longman, Inc., Reading, MA, pp. vii - xii, 7, 8, 1994
18)	Sinclair, C., Pierce, L., and Matzner, S., "*An Application of Machine Learning to Network Intrusion Detection*", The University of Texas at Austin, Austin, TX, pp. 1-7.
19)	Butterworth, J., "*Practical Portion Of Intrusion Detection Immersion Curriculum*", 10 pgs.
20)	Kobi, H., "*Beyond SNMP: The Benefits of Collecting Network Event Logs*", Technical White Paper, Network Intelligence® Corporation, Walpole, MA, pp. 1-10, June 2002.
21)	Harp, S., Geib, C., Goldman, R., Heimerdinger, W., Thomas, V., and R.A. Kemmerer Associates, "*Argus: An Architecture for Cooperating Intrusion Detection and Mitigation Applications*", Honeywell Technology Center, 18 pgs.
22)	Barrus, J. and Rowe, N., "*A Distributed Autonomous-Agent Network-Intrusion Detection and Response System*", Proceedings of the 1998 Command and Control Research and Technology Symposium, Monterey, CA, June - July 1998, 12 pgs.
23)	Frincke, D., Tobin, D., McConnell, J., Marconi, J., and Polla, D., "*A Framework for Cooperative Intrusion Detection*", Center for Secure and Dependable Software, University of Idaho, Moscow, ID, 13 pgs, 1998.
24)	"*Managing Your Network With HP OpenView Network Node Manager*", Hewlett-Packard Company, Fort Collins, CO, pp. 1-675, May 2002.
25)	"*HP OpenView Communications Event Correlation Services Developer's Guide and Reference*", Hewlett-Packard Company, Fort Collins, CO, pp. 1-150, April 2001.
26)	"*HP OpenView Communications Event Correlation Services SNMP Module*", Hewlett-Packard Company, Fort Collins, CO, pp. 1-62, April 2001.
27)	"*HP OpenView Communications Event Correlation Services Administrator's Guide*", Hewlett-Packard Company, Fort Collins, CO, pp. 1-121, April 2001.
28)	Agbabian, P. et al., U.S. Patent Application Serial No. 10/660,422, filed on September 10, 2003, entitled "CONFIGURATION SYSTEM AND METHODS INCLUDING CONFIGURATION INHERITANCE AND REVISIONING", 124 pgs.

A PTO form 1449 listing these documents is enclosed. Citation of the above documents shall not be construed as:

1. an admission that the documents are necessarily prior art with respect to the instant invention;

2. a representation that a search has been made, other than as described above; or

3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 15, 2004.

Attorney for Applicant(s)

June 15, 2004
Date of Signature

Respectfully submitted,

Forrest Gunnison
Attorney for Applicant(s)
Reg. No. 32,899
(831) 655-0880

Sheet 1 of 10

Form PTO-1449 INFORMATION DISCLOSURE CITATION IN AN APPLICATION *(Use several sheets if necessary)*	Atty Docket No. SYMC1001	Serial No. 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	5,893,083	04/06/99	Eshghi et al.	706	45	
	AB	6,266,773 B1	07/24/01	Kisor et al.	713	200	
	AC	6,298,445 B1	10/02/01	Shostack et al.	713	201	
	AD	6,321,338 B1	11/20/01	Porras et al.	713	201	
	AE	6,484,203 B1	11/19/02	Porras et al.	709	224	
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Barrus, J., "*Intrusion Detection in Real Time in a Multi-Node, Multi-Host Environment*", Master's Thesis, Naval Postgraduate School, Monterey, CA, i-xii, pp. 1-79, September 1997.
	AS	Houston, G. et al., U.S. Patent Publication No. US-2002/0019945-A1, published on February 14, 2002, entitled "SYSTEM AND METHOD FOR MANAGING SECURITY EVENTS ON A NETWORK", 29 pgs.
	AT	"*SNIA CIM Interoperability Demonstration Backgrounder*", Storage Networking Industry Association, pp. 1-2, 2002.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 **INFORMATION DISCLOSURE CITATION** **IN AN APPLICATION** *(Use several sheets if necessary)*	Atty Docket No. SYMC1001	Serial No. 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	"*SNIA Storage Management Initiative CIM/WBEM Technology Backgrounder*", Storage Networking Industry Association, pp. 1-2, 2002.
	AS	Hughes, K. and Wohlferd, D., "*Say Goodbye to Quirky APIs: Building a WMI Provider to Expose Your Object Info*", pp. 1-16 [online]. Retrieved on December 24, 2002. Retrieved from the internet: URL:http://msdn.microsoft.com/msdnmag/issues/0500/wmiprov/print.asp.
	AT	"*Common Information Model (CIM) Specification*", Version 2.2, Distributed Management Task Force, Inc., Portland, OR, pp. I-VI, 1-97, June 14, 1999.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 INFORMATION DISCLOSURE CITATION IN AN APPLICATION *(Use several sheets if necessary)*	Atty Docket No. SYMC1001	Serial No. 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Davis, J., "*WBEM Services Specification JSR-0048*", Java One, Sun's 2001 Worldwide Java Developer Conference, pp. 1-19, 2001.
	AS	Bhat, G., "*WBEM Services API and Examples*", Java One, Sun's 2001 Worldwide Java Developer Conference, pp. 20-29, 2001.
	AT	Westerinen, A., "*Modeling Information In CIM*", Java One, Sun's 2001 Worldwide Java Developer Conference, pp. 31-43, 2001.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449	Atty Docket No. SYMC1001	Serial No. 10/660,225
INFORMATION DISCLOSURE CITATION **IN AN APPLICATION**	Applicant(s) Paul M. Agbabian	
(Use several sheets if necessary)	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Ptacek, T. and Newsham, T., "*Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*", Secure Networks, Inc., pp. 1-63, January 1998.
	AS	Yang, J., Ning, P., Wang, X., and Jajodia, S., "*Cards: A Distributed System For Detecting Coordinated Attacks*", Center for Secure Information Systems, George Mason University, Fairfax, VA, pp. 1-10.
	AT	Magers, D., "*Packet Sniffing: An Integral Part of Network Defense*", 9 pgs., May 9, 2002.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 INFORMATION DISCLOSURE CITATION IN AN APPLICATION *(Use several sheets if necessary)*	Atty Docket No. SYMC1001	Serial No. 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	King, N. and Weiss, E., *"Network Forensics Analysis Tools (NFATs) Reveal Insecurities, Turn Sysadmins Into Systems Detectives"*, Information Security, 8 pgs., February 2002.
	AS	Trenum, G., *"Practical Requirement for Level 2 IDIC Exam"*, 15 pgs.
	AT	Shimomura, T., *"Tsutomu Shimomura's Newsgroup Posting With Technical Detail of the Attack Described by Markoff in NYT"*, Random Access, 10 pgs., October 12, 1997.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 **INFORMATION DISCLOSURE CITATION IN AN APPLICATION** *(Use several sheets if necessary)*	Atty Docket No. SYMC1001	Serial No. 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	*"Dragon 5, An Intrusion Detection System for the Enterprise"*, 5 pgs.
	AS	Stevens, W., The Protocols, TCP/IP Illustrated, Volume 1, Addison Wesley Longman, Inc., Reading, MA, pp. vii - xii, 7, 8, 1994
	AT	Sinclair, C., Pierce, L., and Matzner, S., *"An Application of Machine Learning to Network Intrusion Detection"*, The University of Texas at Austin, Austin, TX, pp. 1-7.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449	Atty Docket No. SYMC1001	Serial No. 10/660,225
INFORMATION DISCLOSURE CITATION **IN AN APPLICATION**	Applicant(s) Paul M. Agbabian	
(Use several sheets if necessary)	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Butterworth, J., "*Practical Portion Of Intrusion Detection Immersion Curriculum*", 10 pgs.
	AS	Kobi, H., "*Beyond SNMP: The Benefits of Collecting Network Event Logs*", Technical White Paper, Network Intelligence® Corporation, Walpole, MA, pp. 1-10, June 2002.
	AT	Harp, S., Geib, C., Goldman, R., Heimerdinger, W., Thomas, V., and R.A. Kemmerer Associates, "*Argus: An Architecture for Cooperating Intrusion Detection and Mitigation Applications*", Honeywell Technology Center, 18 pgs.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449	**Atty Docket No.** SYMC1001	**Serial No.** 10/660,225
INFORMATION DISCLOSURE CITATION **IN AN APPLICATION**	**Applicant(s)** Paul M. Agbabian	
(Use several sheets if necessary)	**Filing Date** September 10, 2003	**Group** 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Barrus, J. and Rowe, N., "*A Distributed Autonomous-Agent Network-Intrusion Detection and Response System*", Proceedings of the 1998 Command and Control Research and Technology Symposium, Monterey, CA, June - July 1998, 12 pgs.
	AS	Frincke, D., Tobin, D., McConnell, J., Marconi, J., and Polla, D., "*A Framework for Cooperative Intrusion Detection*", Center for Secure and Dependable Software, University of Idaho, Moscow, ID, 13 pgs, 1998.
	AT	"*Managing Your Network With HP OpenView Network Node Manager*", Hewlett-Packard Company, Fort Collins, CO, pp. 1-675, May 2002.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 **INFORMATION DISCLOSURE CITATION** **IN AN APPLICATION** *(Use several sheets if necessary)*	**Atty Docket No.** SYMC1001	**Serial No.** 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	**Group** 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	*"HP OpenView Communications Event Correlation Services Developer's Guide and Reference"*, Hewlett-Packard Company, Fort Collins, CO, pp. 1-150, April 2001.
	AS	*"HP OpenView Communications Event Correlation Services SNMP Module"*, Hewlett-Packard Company, Fort Collins, CO, pp. 1-62, April 2001.
	AT	*"HP OpenView Communications Event Correlation Services Administrator's Guide"*, Hewlett-Packard Company, Fort Collins, CO, pp. 1-121, April 2001.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 INFORMATION DISCLOSURE CITATION IN AN APPLICATION *(Use several sheets if necessary)*	Atty Docket No. SYMC1001	Serial No. 10/660,225
	Applicant(s) Paul M. Agbabian	
	Filing Date September 10, 2003	Group 2832

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Agbabian, P. et al., U.S. Patent Application Serial No. 10/660,422, filed on September 10, 2003, entitled "CONFIGURATION SYSTEM AND METHODS INCLUDING CONFIGURATION INHERITANCE AND REVISIONING", 124 pgs.
	AS	
	AT	

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).